UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/757,903	01/10/2001	Luis M. Ortiz	K1033	8298

7590 11/23/2007

ORTIZ & LOPEZ, PLLC
Patent Attorney
P. O.4484
Albuquerque,, NM 87196-4484

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
11/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/757,903	ORTIZ, LUIS M.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-12,14-23,25-34 and 36-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 7-12, 14-23, 25-34, and 36-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on September 24, 2007. Claims 1-5, 7-12, 14-23, 25-34, and 36-44 were pending consideration. Per the received amendment, claim 45 was added.

2. Claims 1-5, 7-12, 14-23, 25-34, and 36-45 are currently pending consideration.

Response to Arguments

Applicant's arguments filed September 24, 2007 have been fully considered but they are not persuasive for the following reasons:

Regarding the amended independent claims 1, 22,23, and newly added claim 45, the applicant argues that the Cited Prior Art (CPA), Lewis (U.S. Patent 6,213,391) and Lin et al. (U.S. Patent 6,360,953), does not teach an electronic system adapted to match biometric data obtained wirelessly from a portable device with related biometric data stored in a remote server prior to challenging a user to provide biometrics via a user interface associated with the electronic system for matching with biometric data from at least one of the server on the portable electronic device. However, this aspect of the claims is not found in the specification. There is no comparison of the biometric information before allowing the user to input any biometrics. The comparison of the biometric is, as defined in the specification and the original claims, to determine whether a user is to be allowed to perform a user-desired activity. Therefore, the Examiner asserts that there is no support for the newly added limitations, and the claims are

thereby not enabled by the specification. However, if there was support for the limitations, Lewis still can teach the limitation. Lewis teaches that there are at least two levels of authentication (Lewis: column 5, lines 30-50). In one embodiment of Lewis, unique codes based on the user's unique identification value can be used as a preliminary or secondary verification of identification (Lewis: column 4, liens 41-48). Once the preliminary identification goes through, then the biometric can be entered in to allow the user to input a biometric (Lewis: column 5, lines 1-9). Therefore, it is asserted that the CPA does teach an electronic system adapted to match biometric data obtained wirelessly from a portable device with related biometric data stored in a remote server prior to challenging a user to provide biometrics via a user interface associated with the electronic system for matching with biometric data from at least one of the server on the portable electronic device.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-5, 7-12, 14-23, 25-34, and 36-45 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The claims in the independent claims, that if biometric

attributes from the contactless smart card match biometric attributes from the server, the user is prompted to input a biometric attribute. However, this aspect of the claims is not found in the specification. There is no comparison of the biometric information before allowing the user to input any biometrics. The comparison of the biometric is, as defined in the specification and the original claims, to determine whether a user is to be allowed to perform a user-desired activity, and not to determine whether a user is allowed to enter a randomly selected biometric attribute. Therefore, it is determined that the claims are not enabled by the specification.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 8-12, 14, 16-21, 23, 25-38, 30-34, 36, and 38-43 rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent 6,213,391) in view of Lin et al. (U.S. Patent 6,360,953)

Regarding claim 1, Lewis discloses:

A method for biometrically securing access to an electronic system, said method comprising the steps of:

obtaining identification including biometric attributes of a user using an electronic system associated with a user-desired activity and adapted for supporting communication with portable electronic devices, the identification of said user further retrieved from a portable electronic device associated with said user after said portable electronic device establishes a contactless communication link to support wireless communication between said portable electronic device and said electronic system (column 3 lines 47-65, column 7 lines 36-65), *wherein a biometric input is received by the smart card and used in verifying the identity of an individual*;

accessing a user profile including biometric attributes associated with said user by said electronic system through a computer network from a remote server based on the identification including biometric attributes of said user obtained by said electronic system from said smart card (column 10, lines 8-23), *wherein verifying means may receive a user profile from a central database*;

comparing said identification including biometric attributes obtained by said electronic system from said portable electronic device with said user profile including biometric attributes obtained by said electronic system from said remote server to determine if biometric attributes from said portable electronic device match biometric attributes from said server (Lewis: column 5, lines 30-50), *wherein unique codes based on the user's unique identification value can be used as a preliminary or secondary verification of identification* (Lewis: column 4, liens 41-48) *and once the preliminary identification goes through, then the biometric can be entered in to allow the user to input a biometric* (Lewis: column 5, lines 1-9).

if biometric attributes from said smart card match biometric attributes from said server, prompting said user to input to a biometric user interface associated with said electronic system at least one biometric attribute randomly selected from biometric attributes accessed by said electronic system from at least one of said remote server and said electronic device (column 5 lines 1-9, column 7 lines 36-65), *wherein the system may require the user to speak one of any specific code words previously recorded by the user*; and

permitting said user access to perform a user-desired activity with the electronic system if at least one biometric attribute input by said user to said biometric user interface associated with said electronic system matches said at least one biometric attribute randomly selected by said electronic system from biometric attributes accessed by said electronic system from at least one of said remote server and portable electronic device (column 5 lines 1-9), *wherein if the biometrics of the user match, the user is given access to his account.*

Lewis does not explicitly disclose that the identification is obtained wirelessly through the use of a contactless smart card and a contactless smart card reader. Lin discloses a system wherein a contactless smart card is used to gain access to an restricted area (Lin: column 4, lines 29-44) by comparing fingerprints. This authentication information is wireless transferred to the authorization station which permits the user to gain access (Lin: column 4, lines 43-46). Lewis and Lin are analogous arts in that both use fingerprint data and smart cards to gain access to a restricted area. It would have been

obvious to one of ordinary skill in the art at the time of invention to use a contactless smart card as disclosed by Lin in the system of Lewis because it "affords the relatively high security association with personal print verification without impeding traffic flow through the security check point" (Lin: column 2, lines 65-67).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said computer network is a secure computer network (column 5 lines 64-67, column 9 lines 31-38), *wherein the network can support an ATM transaction.*

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said remote server is a biometric broker (column 10 lines 8-23), *wherein the biometric information may be retrieved from a central database.*

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said portable electronic device is at least one of: smart card, PDA, cellular telephone (column 4, lines 20-25).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Lewis discloses:

The method of claim 4 further comprising the steps of:

permitting the user to modify said user profile, in response to approval of a request by said user *(column 5 lines 31-59), wherein the user can change a PIN in a bank system (column 1 lines 56-57) at any time.*

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises at least one wireless device that operates with a wireless network (column 9 lines 38-46).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises at least one computer workstation operable over an associated network (column 3 lines 47-65).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises an automated teller machine (column 3 lines 47-52).

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises a secured entry system to a secured environment (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate.*

Claim 12 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises a wireless network (column 9 lines 38-46).

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said electronic system comprises a wireless device (column 9 lines 38-46).

Claim 16 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said user-desired activity comprises a financial transaction (column 3 lines 47-52).

Claim 17 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said user-desired activity comprises an ATM transaction (column 3 lines 47-52).

Claim 18 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said user-desired activity comprises access to a secure area (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate.*

Claim 19 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said user-desired activity comprises access to data from said electronic system (column 3 lines 47-52).

Claim 20 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 wherein said user-desired activity comprises execution of a mechanical activity (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate.*

Claim 21 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

The method of claim 1 further comprising the step of:

initiating access to said electronic system utilizing only one biometric input to said electronic system (column 8 lines 7-15).

Regarding claim 23, Lewis discloses:

A system for biometrically securing access to a user-desired activity and said system comprising:

a biometric user interface (column 4 lines 27-64);

ii) communicate with remote servers

iii) compare user identification including biometric attributes obtained by said electronic system from a portable electronic device with a user profile including biometric attributes obtained by said electronic system from a remote server to determine if biometric attributes obtained from said smart card match biometric attributes obtained from said server (column 5 lines 1-9), *wherein if the biometrics of the user match, the user is given access to his account*, iv) receive biometric attributes obtained from said server (column 5 lines 1-9), *wherein if the biometrics of the user match, the user is given access to his account;* iv) receive biometric attributes from a user through said biometric user interface (column 5 lines 1-9) and v) permit a user to perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches said at least one biometric attribute randomly selected from a remote server based on identification of a user obtained from a smart card in communication with a card reader associated with the electronic system (column 5 lines 1-9, column 7 lines 36-65), wherein said smart card is adapted to store at least one user profile including biometric attributes and provide said electronic system access to at

least one user profile (column 3 lines 47-65, column 7 lines 36-65), *wherein a biometric input is received by the smart card and used in verifying the identity of an individual.*

Lewis does not explicitly disclose that the identification is obtained wirelessly through the use of a contactless smart card and a contactless smart card reader. Lin discloses a system wherein a contactless smart card is used to gain access to an restricted area (Lin: column 4, lines 29-44) by comparing fingerprints. This authentication information is wireless transferred to the authorization station which permits the user to gain access (Lin: column 4, lines 43-46). Lewis and Lin are analogous arts in that both use fingerprint data and smart cards to gain access to a restricted area. It would have been obvious to one of ordinary skill in the art at the time of invention to use a contactless smart card as disclosed by Lin in the system of Lewis because it "affords the relatively high security association with personal print verification without impeding traffic flow through the security check point" (Lin: column 2, lines 65-67).

Claim 25 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user profile is accessible from a biometric broker via a secure network connection (column 10 lines 8-23), *wherein the biometric information may be retrieved from a central database.*

Claim 26 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein:

wherein said remote server is a biometric broker (column 4 lines 40-57), *wherein at the time an account is opened, the user provides biometric input to be stored on the smart card and/or the database.*

Claim 27 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said biometric user interface is adapted to accept at least one of the following attributes from a user: fingerprint, iris, voice, signature, facial, hand geometry, retinal, palm, ear DNA, keystroke, body odor (column 4, lines 50-56).

Claim 28 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 further comprising:

module for comparing at least one biometric attribute input by said user to said biometric user interface associated with said electronic system with said at least one biometric attribute randomly selected from said user profile (column 5 lines 1-9), *wherein if the biometrics of the user match, the user is given access to his account.*

Claim 30 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said electronic system comprises at least one wireless device that operates with a wireless network (column 9 lines 38-46).

Claim 31 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said electronic system comprises at least one computer workstation accessible over said computer network (column 3 lines 47-65).

Claim 32 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said electronic system comprises an automated teller machine (column 3 lines 47-52).

Claim 33 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said electronic system comprises a secured entry system to a secured environment (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate.*

Claim 34 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said computer network comprises a wireless network (column 9 lines 38-46).

Claim 36 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said electronic system comprises a wireless device, a contactless smart card, a PDA, a cellular phone (column 9 lines 38-46).

Claim 38 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user-desired activity comprises a financial transaction (column 3 lines 47-52).

Claim 39 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user-desired activity comprises an ATM transaction (column 3 lines 47-52).

Claim 40 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user-desired activity comprises access to a secure area (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate.*

Claim 41 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user-desired activity comprises access to data from said electronic system (column 3 lines 47-52).

Claim 42 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein said user-desired activity comprises execution of a mechanical activity (column 3 lines 47-52), *wherein the electronic system could allow entry through a security gate.*

Claim 43 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

The system of claim 23 wherein access to said electronic system is initiated utilizing only one biometric attribute input to said electronic system (column 8 lines 7-15).

Regarding claim 45, Lewis discloses:

A system for biometrically securing access to a user-desired activity, said system comprising:

a biometric user interface electronically associated with an electronic system adapted to:

communicate with smart cards (column 3, lines 47-65, column 7, lines 36-65), *wherein a biometric input is received by the smart card and used in verifying the identity of an individual*;

communicate with remote servers (column 10, lines 8-23), *wherein verifying means may receive a user profile from a central database*;

compare user identification including biometric attributes obtained by said electronic system from a smart card with a user profile including biometric attributes obtained by said electronic system from a remote server to determine if biometric attributes obtained from said smart card match biometric attributes obtained from said server (Lewis: column 5, lines 30-50), *wherein unique codes based on the user's unique identification value can be used as a preliminary or secondary verification of identification* (Lewis: column 4, liens 41-48) *and once the preliminary identification goes through, then the biometric can be entered in to allow the user to input a biometric* (Lewis: column 5, lines 1-9).;

receive biometric attributes from a user through said biometric user interface (column 5, lines 1-9, column 7, liens 36-65), *wherein the system may require the user to speak any specific code word previously recorded by the user*; and

permit a user to perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches at least one biometric attribute randomly selected by said electronic system from at least one of a user profile including biometric attributes associated with said user accessible by the electronic system from a remote server and based on identification including biometric attributes associated with said user obtained from a smart card in communication with a card reader with the electronic system if said electronic system determines that biometric attributes associated with said user obtained from said remote server match biometric attributes associated with said user obtained from said contactless card (column 5, lines 1-9), *wherein if the biometrics of the user match, the user is given access to his account* and (Lewis: column 5, lines 30-50), *wherein unique codes based on the user's unique identification value can be used as a preliminary or secondary verification of identification* (Lewis: column 4, liens 41-48) *and once the preliminary identification goes through, then the biometric can be entered in to allow the user to input a biometric* (Lewis: column 5, lines 1-9).

6. Claims 7, 15, 29, 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent 6,213,391) in view of Lin et al. (U.S. Patent 6,360,953) in view of Price-Francis (U.S. Patent 5,815,252).

Claim 7 is rejected as applied above in rejecting claim 6. Lewis-Lin does not explicitly disclose subsequently prompting a user to input another biometric input if the at least one biometric attribute does not match the one randomly selected from the user profile. Price-Francis discloses subsequently prompting a user to input another biometric if at least one previously input biometric does not match the randomly selected biometric in the user profile (column 6 lines 59- column 7 line 4). Lewis and Price-Francis are analogous arts in that both use biometrics to authenticate a user before allowed the user to perform a secured activity. It would have been obvious to modify the system of Lewis to provide another input of biometrics if the first failed to authenticate for "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

Claim 15 is rejected as applied above in rejecting claim 6. Lewis does not explicitly disclose subsequently prompting a user to input another biometric input if the at least one biometric attribute does not match the one randomly selected from the user profile. Price-Francis discloses subsequently prompting a user to input another biometric if at least one previously input biometric does not match the randomly selected biometric in the user profile (column 6 lines 59- column 7 line 4). Lewis and Price-Francis are analogous arts in that both use biometrics to authenticate a user before allowed the user to perform a secured activity. It would have been obvious to modify the system of

Lewis to provide another input of biometrics if the first failed to authenticate for "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

Claim 29 is rejected as applied above in rejecting claim 28. Lewis does not explicitly disclose subsequently prompting a user to input another biometric input if the at least one biometric attribute does not match the one randomly selected from the user profile. Price-Francis discloses subsequently prompting a user to input another biometric if at least one previously input biometric does not match the randomly selected biometric in the user profile (column 6 lines 59- column 7 line 4). Lewis and Price-Francis are analogous arts in that both use biometrics to authenticate a user before allowed the user to perform a secured activity. It would have been obvious to modify the system of Lewis to provide another input of biometrics if the first failed to authenticate for "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

Claim 37 is rejected as applied above in rejecting claim 23. Lewis does not explicitly disclose subsequently prompting a user to input another biometric input if the at least

one biometric attribute does not match the one randomly selected from the user profile. Price-Francis discloses subsequently prompting a user to input another biometric if at least one previously input biometric does not match the randomly selected biometric in the user profile (column 6 lines 59- column 7 line 4). Lewis and Price-Francis are analogous arts in that both use biometrics to authenticate a user before allowed the user to perform a secured activity. It would have been obvious to modify the system of Lewis to provide another input of biometrics if the first failed to authenticate for "allowing for comparison of two or more fingerprints, the possibility of a defective signal based on an obscured or unavailable fingerprint, environmental factors, such as excess moisture on the fingers, or any artifact preventing a match from being made, can be compensated for" (column 6 line 59 – column 7 line 4).

7. Claims 22, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent 6,213,391) in view of Lin et al. (U.S. Patent 6,360,953) further in view of Abrahams (U.S. Patent 6,944,773).

Regarding claim 22, Lewis discloses:

A method for biometrically securing access to a secure area, said method comprising the steps of:

obtaining identification of a user by an electronic system using a a card reader in communication with said electronic system, the identification of said user further retrieved from a smart card(column 3 lines 47-65, column 7 lines 36-65), *wherein a*

biometric input is received by the smart card and used in verifying the identity of an individual;

said electronic system using a computer network to obtain a user profile associated with said user from a remote server, said user profile including biometric attributes (column 4 lines 55-57, column 10 lines 10-22), *wherein the profile can be fetched from a central database*;

comparing said identification including biometric attributes obtained by said electronic system from said portable electronic device with said user profile including biometric attributes obtained by said electronic system from said remote server to determine if biometric attributes from said portable electronic device match biometric attributes from said server (Lewis: column 5, lines 30-50), *wherein unique codes based on the user's unique identification value can be used as a preliminary or secondary verification of identification* (Lewis: column 4, liens 41-48) *and once the preliminary identification goes through, then the biometric can be entered in to allow the user to input a biometric* (Lewis: column 5, lines 1-9).

if biometric attributes from said smart card match biometric attributes from said server, prompting said user to input to a biometric user interface associated with said electronic system at least one biometric attribute randomly selected from biometric attributes accessed by said electronic system from at least one of said remote server and said electronic device (column 5 lines 1-9, column 7 lines 36-65), *wherein the system may require the user to speak one of any specific code words previously recorded by the user*; and

permitting said user access to perform a user-desired activity with the electronic system if at least one biometric attribute input by said user to said biometric user interface associated with said electronic system matches said at least one biometric attribute randomly selected by said electronic system from biometric attributes accessed by said electronic system from at least one of said remote server and portable electronic device (column 5 lines 1-9), *wherein if the biometrics of the user match, the user is given access to his account;*

said electronic system prompting said user to input into a biometric user interface associated with said electronic system at least one biometric attribute randomly selected by said electronic system

Lewis does not explicitly disclose that the identification is obtained wirelessly through the use of a contactless smart card and a contactless smart card reader. Lin discloses a system wherein a contactless smart card is used to gain access to an restricted area (Lin: column 4, lines 29-44) by comparing fingerprints. This authentication information is wireless transferred to the authorization station which permits the user to gain access (Lin: column 4, lines 43-46). Lewis and Lin are analogous arts in that both use fingerprint data and smart cards to gain access to a restricted area. It would have been obvious to one of ordinary skill in the art at the time of invention to use a contactless smart card as disclosed by Lin in the system of Lewis because it "affords the relatively high security association with personal print verification

without impeding traffic flow through the security check point" (Lin: column 2, lines 65-67).

Lewis-Lin does not explicitly mention randomly selecting at least one biometric attribute by said electronic system from the user profile. Abrahams discloses prompting a user for two or more biometric attributes (fingerprints), which are randomly selected, and if the fingerprints match, authenticating the user to perform a task (column 3 lines 27-50). Abrahams and Lewis are analogous arts in that both use biometric attributes to authenticate a user to perform a task including financial transactions. Allowing the system of Lewis to check for multiple biometrics would be feasible as the smart card and the biometric database of Lewis store multiple biometric attributes of each user (column 5 lines 1-9). It would have been obvious to one of ordinary skill in the art at the time of invention to prompt the user for randomly selected biometric attributes before authenticating the user so that the likelihood of fraud is reduced (Abrahams: column 4 lines 15-22, column 4 lines 57-59).

Regarding claim 44, Lewis discloses:

A system for biometrically securing access to an electronic system, said system comprising:

an electronic system adapted to permit a user to perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches said at least one biometric attribute randomly selected from said user profile accessible by the electronic system over a computer network from a remote server, said

electronic system including access to a remote server through electronic connection to a computer network and said remote server adapted to store at least one user profile including biometric attributes and provide said electronic system to said at least one user profile (column 4 lines 55-57, column 10 lines 10-22), *wherein the profile can be fetched from a central database.*;

Lewis does not explicitly disclose that the identification is obtained wirelessly through the use of a contactless smart card and a contactless smart card reader. Lin discloses a system wherein a contactless smart card is used to gain access to an restricted area (Lin: column 4, lines 29-44) by comparing fingerprints. This authentication information is wireless transferred to the authorization station which permits the user to gain access (Lin: column 4, lines 43-46). Lewis and Lin are analogous arts in that both use fingerprint data and smart cards to gain access to a restricted area. It would have been obvious to one of ordinary skill in the art at the time of invention to use a contactless smart card as disclosed by Lin in the system of Lewis because it "affords the relatively high security association with personal print verification without impeding traffic flow through the security check point" (Lin: column 2, lines 65-67).

Lewis-Lin does not explicitly mention randomly selecting at least one biometric attribute by said electronic system from the user profile. Abrahams discloses prompting a user for two or more biometric attributes (fingerprints), which are randomly selected, and if the fingerprints match, authenticating the user to perform a task (column 3 lines

27-50). Abrahams and Lewis are analogous arts in that both use biometric attributes to authenticate a user to perform a task including financial transactions. Allowing the system of Lewis to check for multiple biometrics would be feasible as the smart card and the biometric database of Lewis store multiple biometric attributes of each user (column 5 lines 1-9). It would have been obvious to one of ordinary skill in the art at the time of invention to prompt the user for randomly selected biometric attributes before authenticating the user so that the likelihood of fraud is reduced (Abrahams: column 4 lines 15-22, column 4 lines 57-59).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

K.A. 11/18/07

KA
11/18/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100